

REMARKS/ARGUMENTS

Applicant respectfully requests reconsideration and allowance of the subject application.

Claims 1-21 were originally submitted.

Claims 11-21 are withdrawn without prejudice per a Restriction Requirement of an earlier communication.

No claims are amended in this response.

No new claims are added.

Claims 1-10 remain in this application.

35 U.S.C. §102

Claims 1, 4, 5 and 8 have been rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,141,423 to Fischer (Fischer). Applicant respectfully traverses the rejection.

In order to prevent the transfer of any escrowed information within a computer to some body other than a legitimate owner, Fischer teaches a method that employs a voluntary identification/definition performed after a computer is purchased, and a secret information retrieval phase. The escrowed information is any information stored on a computer which has been encrypted through a third party encryption. See Fischer, col. 1, lines 42-52.

In particular, the mechanisms taught by Fischer include third party authentication and verification for determining the ownership of the escrowed information. In the definition phase, the true owner/customer defines an escrow record that provides self identification data together with encrypted password or any other secret data. The identification indicia is combined with the secret

information (e.g., the user's encryption password) and is encrypted under the control of a trustee's public key. As the user enters the unique identification data, he is asked to select a password to protect the system. Thereafter, all the personal identifying data together with the password is encrypted with the manufacturer's (trustee's) public key and is stored in the user's computer as an escrow security record. The secret information retrieval phase of the invention is of use in cases when the user forgets his/her password. See Fischer, col.2, lines 41-67; col.10, lines 14-53; Fig.6; Col. 12, lines 13-18.

Fig. 6 of Fishers shows a flowchart of a sequence of operations performed when an applicant attempts to retrieve escrowed secret information. The applicant may either be a legitimate owner of the information or a person attempting to steal valuable information. The applicant initially provides the trustee with the escrow information record which has been encrypted with the trustee's public key. The applicant further presents the trustee with the documentation containing credentials that can be matched with the escrowed information. The request for the secret information must be verifiable with the same public key that is in the escrow record. Moreover, the physical appearance of the applicant must match the described characteristics in the standard identifying information. The trustee performs a matching of the hash value of the escrow record with the hash value supplied to him by the applicant. If these values match, the trustee is assured that the escrow record has been delivered in the correct form. Based on these criteria, the trustee determines whether the applicant is a legitimate owner or someone who has a genuine claim to the data.

1 If the applicant turns out to be a legitimate owner, the secret information is
2 provided to him and he decrypts the supplied secret escrowed information using
3 the appropriate private key.

4 **Independent claim 1**, recites “[a] computer-implemented method
5 comprising:

6 sending a request for network account credentials from an
7 originating account associated with an unpublished object at a dispatch
8 associated with a published object, the request directed to the published
9 object associated with the dispatch includes identification of the
10 unpublished object associated with the originating account;

11 authenticating the originating account at the dispatch; and,

12 upon authenticating the originating account, sending an emblem that
13 includes an object and credential, for a network account to the originating
14 account, the emblem sent to the unpublished object associated with the
15 originating account and having the identification as included with the
16 request.

17 Fischer does not disclose “upon authenticating the originating account,
18 sending an emblem that includes an object and credential for a network account to
19 the originating account, the emblem sent to the unpublished object associated with
20 the originating account and having the identification as included with the request.”
21 as recited in claim 1.

22 As discussed above, Fischer discloses a transfer of decrypted escrow
23 information along with secret credentials once authentication is successful. The
24 transferred escrow information includes only decrypted information and is used
25

1 essentially by a trustee in the process of identifying whether an applicant of secret
2 information is the legitimate user.

3 Fischer discloses that during authentication of an applicant, some
4 information is required about the applicant. Preferably this information is stored
5 on the applicant's computer in an encrypted manner. This information is referred
6 to as an escrow record and further includes a field that secretly holds a key which
7 can decrypt entire data stored on the applicant's computer. Whenever an applicant
8 requires secret credentials to decrypt entire data on his computer he sends the
9 encrypted escrow record to the trustee. The trustee in turn decrypts the escrowed
10 record to establish that the applicant is the legitimate owner of the information and
11 to retrieve the secret key stored on the escrow record. Once the determination is
12 done the trustee sends the secret credentials along with the decrypted escrow
13 record to the applicant. See Fischer, col.8, lines 6-35; col.10, lines 14-55; col. 12,
14 lines 12-18.

15 In contrast, the application describes a transfer of an emblem which
16 contains a secret credential and an object. The object is capable of storing data
17 and instructions, it can include files, message queues etc. For example, see
18 specification page 13 line 21 to page 14 line 3. The object generally stores
19 instructions assigned by a dispatch which are to be done to accomplish batch
20 processing. It is further disclosed that the emblem can be used to store and transfer
21 both instructions for batch processing and credentials to access information
22 required to carry out the instructions. There is no mention of such a transfer of an
23 emblem in Fischer stores and transfers both credentials and object.

24 Correspondingly, Fischer does not disclose "upon authenticating the
25 originating account, sending an emblem that includes an object and credential for a

1 network account to the originating account, the emblem sent to the unpublished
2 object associated with the originating account and having the identification as
3 included with the request” as recited in claim 1. We therefore believe that
4 successful arguments can be made on these bases to overcome the Office’s
5 rejection of independent claim 1.

6 Accordingly, Fischer does not show every element of claim 1, and the
7 rejection of claim 1 is therefore improper. Accordingly, Applicant respectfully
8 request that the §102 rejection of claim 1 be withdrawn.

9 **Dependent claims 4, 5 and 8** depend from claim 1, and are allowable at the
10 least for reasons provided in support of claim 1. Accordingly, Applicant
11 respectfully request that the §102 rejection of claims 4, 5 and 8 be withdrawn.

12 Claim 8 further recites “wherein the network account for which the emblem
13 is sent from the dispatch to the originating account comprises an agent account of
14 an agent”.

15 Fischer teaches transferring a secret decryption key to a user once it is
16 determined that the user is the legitimate owner of the escrowed information.
17 There is no mention of sending an emblem from the central authority (dispatch) to
18 the originating account (requesting user) includes an agent account of an agent.
19 Fischer teaches a transfer of a secret decryption key to field a request from a user.
20 Furthermore, the request is made by the user to retrieve the coded escrowed
21 information which can be decrypted only by the secret key residing with a third
22 party (escrow trustee). Additionally, the communication is directly between the
23 trustee and the user requesting the decryption key. The mechanism suggested by
24 Fischer is just a validation and authentication procedure to ensure that the
25

1 requesting user is a legitimate owner of the escrowed information. See Fischer,
2 col. 11, lines 4-16; col. 12, lines 12-18.

3 The Application discloses a mechanism where an emblem is sent from the
4 central authority (dispatch) to the requesting user (originating account) through an
5 agent account of an agent. For example, see Application, page 11, lines 10-22;
6 page 12 line 20 through page 13 line 5. The central authority uses an agent
7 account in a situation that requires grant of global access privileges to more than
8 one client computer on a distributed network. During batch processing over a
9 distributed network it may be required that global access rights, normally assigned
10 to only network accounts like that of a central authority (dispatch) should be given
11 to client computers involved on batch processing. The central authority may be
12 allowed to simultaneously grant global access rights to more than one originating
13 accounts. In particular, the central authority transfers it's rights to the originating
14 accounts through proxy logging onto the agent accounts and then remoting to the
15 originating accounts. In comparison, Fischer fails to teach or disclose fielding
16 requests of originating accounts by transfer of emblems through agent accounts.

17
18 **35 U.S.C. §103**

19 Claims 2, 3 and 4 have been rejected under 35 U.S.C. 103(a) as being
20 unpatentable by Fischer. Applicant respectfully traverses the rejection.

21 **Claims 2, 3 and 4** depend on claim 1 and are allowable based on arguments
22 presented above in support of claim 1. Accordingly, Applicant respectfully request
23 that the §103 rejection of claims 2, 3 and 4 be withdrawn.

24 Claims 6 and 7 have been rejected under 35 U.S.C. 103(a) as being
25 unpatentable over Fischer as applied to independent claim 1 and further in view of

1 US patent No. 5,613,012 issued to Hoffman et al. (Hoffman). Applicant
2 respectfully traverses the rejection.

3 **Claims 6 and 7** depend on claim 1 and are allowable based on arguments
4 presented above in support of claim 1. Accordingly, Applicant respectfully request
5 that the §103 rejection of claims 6 and 7 be withdrawn.

6 Claim 9 has been rejected under 35 U.S.C. 103(a) as being unpatentable
7 over Fischer as applied to claim 1 and further in view of US patent No. 5974566
8 issued to Ault et al. (Ault). Applicant respectfully traverses the rejection.

9 **Claim 9** depends on claim 1 and is allowable based on arguments presented
10 above in support of claim 1. Accordingly, Applicant respectfully request that the
11 §103 rejection of claim 9 be withdrawn.

12 Claim 10 has been rejected under 35 U.S.C. 103(a) as being unpatentable
13 over Fischer as applied to claim 1 and further in view of US patent No. 6,006,018
14 issued to Burnett et al. (Burnett). Applicant respectfully traverses the rejection.

15 **Claim 10** depends on claim 1 and is allowable based at least on arguments
16 presented above in support of claim 1.

17 Claim 10 further recites "wherein the emblem is expirable, such that the
18 method further comprises determining whether the emblem is about to expire, and
19 upon so determining, renewing the emblem with a renewing authority."

20 Burnett fails to teach or suggest this element. Burnett teaches a mechanism
21 to restore mapping upon expiration of an authentication period of mapping
22 between different file systems. In general, Burnett teaches a mechanism to
23 facilitate interoperability and coexistence of different distributed file systems
24 within a distributed computing environment (DCE) domain. This is achieved by
25 mapping credentials associated with a requesting user into credentials containing

1 authentication information associated with a target distributed file system's
2 authentication model or paradigm. Subsequently, a connection is established
3 between the requesting user and the target file system through a VFS (virtual file
4 system) switch. Burnett further teaches that a user in a DCE can determine when
5 his/her credentials will expire using a Klist command; however, Burnett admits
6 this determination cannot be done in a NFS/DFS translator model because there is
7 not a running process on the translator system which DCE credentials can be
8 associated with to perform the Klist command. Therefore, a translator user cannot
9 list his credential information. Furthermore, Burnett admits that the user is not
10 notified when his/her mapping has expired. Moreover, when DCE credentials
11 expire a translator user is not able to renew his credentials. See Burnett, col.22,
12 lines 19-46; col.1, lines 48-67; col.2, lines 1-17 ; col.2, lines 53-67).

13 The application describes a mechanism in which the emblems are expirable,
14 such that they are only valid for a limited period of time, to add another level of
15 security within the system. When the emblem is about to expire, it is renewed with
16 a renewing authority so that the originator that is the holder of the emblem can
17 continue to access system resources as allowed by the network access credentials
18 encased within the emblem. See for example, Application, page 17, lines 20-23
19 through page 18 lines 1-3; page 14, lines 20-23 ; page 15, lines 1-4. Burnett
20 teaches a mechanism to determine credential mapping status.

21
22
23
24
25

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25

- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25

8

10

10

11